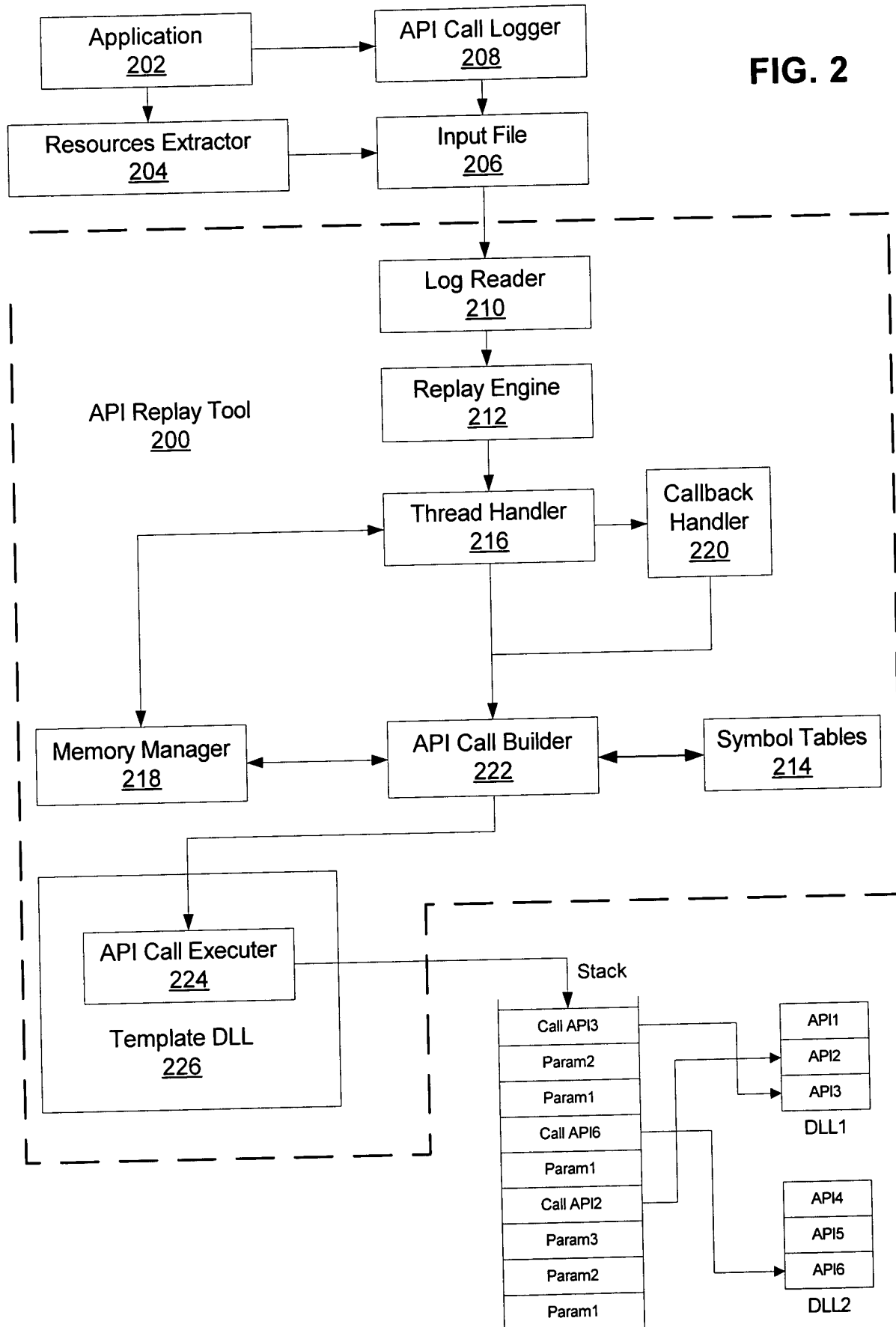


FIG. 1



300	API Call Fields
	API ID
	Thread ID
	Process ID
	API Name
	API Calling Module Name (ex: cards.dll)
	API Calling Module ID (an ID to be given at recording time)
	API Called Module Name (ex: user32.dll, kernel32.dll)
	API Called Module ID
	Depth (nesting level)
	Time Stamp
	API's GLE
	Failure/exception info.
330	API Parameters (one set per parameter)
	Size
	Type (ID and Name)
	Base Type (ID and Name)
	Array Size
	Indirection Count
	Modifier (In, Out, In/Out)
	Number of members (for structures)
	GUID
	Parameters to be retrieved
	Verification values
	Attached values
	Flags
360	Operating System Message
	Message ID
	Message Type (user/system)
	LParam and WParam
	Time Stamp
	Handle
390	Resources to be Retrieved

FIG. 3

400	Initialize
402	RunLog
404	CreateInitialProcess
406	CreateInitialThread
408	HandleSpecialAPI
410	IsFilteredAPI
412	GetFirstLogRecord
414	GetNextAPICode
416	GetNextLogRecord
418	GetNextBlockCode
420	GetNextSegmentCode
422	GetInterface(*)

FIG. 4

500	Memory Manager
510	Process Block
520	Thread Block
530	Memory Block
540	Code Data

FIG. 5

FIG. 6

